IN THE CLAIMS:

4. (Once amended) [The method of Claim 2,] A method for privately communicating over a wireless communications network, comprising the steps of:

processing the communication signals in a first signal processing circuit within a first communications controller circuit at a first location to produce processed communication signals;

enciphering the processed communication signals in the first signal processing circuit at said first location to produce enciphered and processed communication signals;

transmitting the enciphered and processed communication signals between a first location and a second location using the first communications controller circuit at said first location;

receiving the enciphered and processed communication signals at the second location using a second communications controller circuit;

deciphering the enciphered and processed communication signals in a second signal processing circuit within the second communications controller circuit at said second location; and

processing the deciphered and processed communication signals in the second signal processing circuit to produce communications signals at the second location;

[wherein said enciphering step comprises the step of embedding the enciphering algorithm in said first signal processing circuit] wherein said enciphering step further comprises the steps of:

B1 cont

embedding an enciphering algorithm within the first signal processing circuit after manufacturing said first communications controller circuit**; and**

enciphering the processed communication signals using the embedded enciphering algorithm.

6. **(Once amended)** The method of Claim **4** [2], wherein said enciphering algorithm embedding step comprises the step of embedding an F enciphering algorithm in said first signal processing circuit.

B2

7. **(Once amended)** The method of Claim **4** [2], wherein said enciphering algorithm embedding step comprises the step of embedding a DES enciphering algorithm in said first signal processing circuit.

8. **(Once amended)** The method of Claim **4** [2], wherein said enciphering algorithm embedding step comprises the step of embedding a BONUS enciphering algorithm in said first signal processing circuit.

9. **(Once amended)** The method of Claim **4** [2], wherein said enciphering algorithm embedding step comprises the step of embedding a DECT standard enciphering algorithm in said first signal processing circuit.

36

10. (Once amended) [The method of Claim 1,] A method for privately communicating over a wireless communications network, comprising the steps of:

processing the communication signals in a first signal processing circuit within a first communications controller circuit at a first location to produce processed communication signals;

B2 cont

enciphering the processed communication signals in the first signal processing circuit at said first location to produce enciphered and processed communication signals;

transmitting the enciphered and processed communication signals between a first location and a second location using the first communications controller circuit at said first location;

receiving the enciphered and processed communication signals at the second location using a second communications controller circuit;

deciphering the enciphered and processed communication signals in a second signal processing circuit within the second communications controller circuit at said second location; and

processing the deciphered and processed communication signals in the second signal processing circuit to produce communications signals at the second location;

wherein said enciphering step further comprises the step of enciphering said processed communication signals in said first signal processing circuit by programmably selecting an enciphering algorithm.

B3

12. **(Once amended)** The method of Claim 10, wherein said deciphering step further comprises the step of deciphering the processed communication signals in a dedicated signal

B3 cont

processing unit of the **[first]** **second** signal processing circuit, the dedicated signal processing unit being tasked to perform said deciphering step.

13. **(Once amended) [The method of Claim 1,] A method for privately communicating over a wireless communications network, comprising the steps of:**

B4

processing the communication signals in a first signal processing circuit within a first communications controller circuit at a first location to produce processed communication signals;

enciphering the processed communication signals in the first signal processing circuit at said first location to produce enciphered and processed communication signals;

transmitting the enciphered and processed communication signals between a first location and a second location using the first communications controller circuit at said first location;

receiving the enciphered and processed communication signals at the second location using a second communications controller circuit;

deciphering the enciphered and processed communication signals in a second signal processing circuit within the second communications controller circuit at said second location; and

processing the deciphered and processed communication signals in the second signal processing circuit to produce communications signals at the second location;

wherein said deciphering step comprises the step of embedding **[said] a** deciphering algorithm in said second signal processing circuit after manufacturing said **[first] second** communications controller circuit.

B5

16. **(Once amended)** The method of Claim 13, wherein said **[enciphering] deciphering** algorithm embedding step comprises

B5 cont

the step of embedding a DECT standard enciphering algorithm in said **[first]** **second** signal processing circuit.

40

18. **(Once amended) [The method of Claim 1,] A method for privately communicating over a wireless communications network, comprising the steps of:**

processing the communication signals in a first signal processing circuit within a first communications controller circuit at a first location to produce processed communication signals;

enciphering the processed communication signals in the first signal processing circuit at said first location to produce enciphered and processed communication signals;

B6

transmitting the enciphered and processed communication signals between a first location and a second location using the first communications controller circuit at said first location;

receiving the enciphered and processed communication signals at the second location using a second communications controller circuit;

deciphering the enciphered and processed communication signals in a second signal processing circuit within the second communications controller circuit at said second location; and

processing the deciphered and processed communication signals in the second signal processing circuit to produce communications signals at the second location; and

[further comprising the step of] generating authentication signals from said first location, comprising performing in said first signal processing circuit the steps of:

generating a first location identifier;

receiving a randomly generated number from said second location;

41

employing a privacy function on said randomly generated number and said first location identifier to generate an enciphered value; and

directing said enciphered value to said second communications controller circuit.

B6 cont

19. **(Once amended)** The method of Claim **18** **[1]**, further comprising the step of authenticating said communication signals from said first location, said authenticating step comprising performing in said second signal processing circuit the steps of:

generating **[said]** **a** first location identifier;

randomly generating **[said]** **a** randomly generated number;

employing a privacy function on said randomly generated number and said first location identifier to generate an expected enciphered value;

receiving said enciphered value from said first location;

comparing said expected enciphered value to said enciphered value; and

generating an authentication signal in the event that said expected enciphered value matches said enciphered value.

42

20. (Once amended) [The method of Claim 1,] A method for privately communicating over a wireless communications network, comprising the steps of:

processing the communication signals in a first signal processing circuit within a first communications controller circuit at a first location to produce processed communication signals;

enciphering the processed communication signals in the first signal processing circuit at said first location to produce enciphered and processed communication signals;

transmitting the enciphered and processed communication signals between a first location and a second location using the first communications controller circuit at said first location;

receiving the enciphered and processed communication signals at the second location using a second communications controller circuit;

deciphering the enciphered and processed communication signals in a second signal processing circuit within the second communications controller circuit at said second location; and

processing the deciphered and processed communication signals in the second signal processing circuit to produce communications signals at the second location; and

further comprising the step of XOR-ing said enciphered and processed communication signals with clear processed communication signals for preventing propagation of single-bit errors from said first signal processing circuit to said second signal processing circuit.

B6 cont

43

21. **(Twice amended)** A system for privately communicating communications signals over a wireless communications network, comprising:

a first communications controller at a first location;

a first signal processing circuit within **[a]** **said** first communications controller circuit at **[a]** **the** first location for processing communications signals to form processed communication signals and further **for** enciphering said processed communication signals;

B6 cont

a first transceiver associated at said first location with said first communications controller for transmitting said enciphered and processed communication signals between said first location and a second location;

a second communications controller circuit at the second location for controlling communications at said second location;

a second transceiver associated at the second location with said second communications circuit for receiving said enciphered and processed communication signals from said first transceiver;

a second signal processing circuit within said second communications controller circuit at the second location for deciphering said received enciphered and processed communication signals, said second signal processing circuit further for processing said deciphered and processed communication signals.

44

27. (Once amended) [The system of Claim 22,] A system for privately communicating communications signals over a wireless communications network, comprising:

a first communications controller at a first location;

a first signal processing circuit within [a] said first communications controller circuit at [a] the first location for processing communications signals to form processed communication signals and further for enciphering said processed communication signals;

a first transceiver associated at said first location with said first communications controller for transmitting said enciphered and processed communication signals between said first location and a second location;

B3

a second communications controller circuit at the second location for controlling communications at said second location;

a second transceiver associated at the second location with said second communications circuit for receiving said enciphered and processed communication signals from said first transceiver;

a second signal processing circuit within said second communications controller circuit at the second location for deciphering said received enciphered and processed communication signals, said second signal processing circuit further for processing said deciphered and processed communication signals;

wherein said first signal processing circuit comprises a first digital signal processing circuit; and

wherein said first signal processing circuit further comprises circuitry and instructions for embedding said enciphering algorithm in said first signal processing circuit

45

after first manufacturing said first communications controller circuit.

B7 cont

28. **(Once amended)** The system of Claim **27** **[23]**, wherein said first signal processing circuit comprises circuitry and instructions for embedding an F enciphering algorithm in said first signal processing circuit.

29. **(Once amended)** The system of Claim **27** **[23]**, wherein said first signal processing circuit comprises circuitry and instructions for embedding a DES enciphering algorithm in said first signal processing circuit.

30. **(Once amended)** The system of Claim **27** **[23]**, wherein said first signal processing circuit comprises circuitry and instructions for embedding a BONUS enciphering algorithm in said first signal processing circuit.

31. **(Once amended)** The **[method]** **system** of Claim **27** **[23]**, wherein said **first signal processing circuit comprises circuitry and instructions for** **[enciphering algorithm embedding step comprises the step of]** embedding a DECT standard enciphering algorithm in said first signal processing circuit.

46

33. (Once amended) [The system of Claim 23,] A system for privately communicating communications signals over a wireless communications network, comprising:

a first communications controller at a first location;

a first signal processing circuit within said first communications controller circuit at the first location for processing communications signals to form processed communication signals and further for enciphering said processed communication signals;

B8

a first transceiver associated at said first location with said first communications controller for transmitting said enciphered and processed communication signals between said first location and a second location;

a second communications controller circuit at the second location for controlling communications at said second location;

a second transceiver associated at the second location with said second communications circuit for receiving said enciphered and processed communication signals from said first transceiver;

a second signal processing circuit within said second communications controller circuit at the second location for deciphering said received enciphered and processed communication signals, said second signal processing circuit further for processing said deciphered and processed communication signals.

wherein said first signal processing circuit comprises a first digital signal processing circuit; and

further comprising a dedicated digital signal processor within said first digital signal processing circuit for enciphering said processed communication signals;

wherein said first signal processing circuit comprises circuitry and instructions for enciphering said processed

B8 cont

communication signals in said first signal processing circuit by programmably selecting an enciphering algorithm.

34. **(Once amended)** The system of Claim **33** **[29]**, said first signal processing circuit further comprises circuitry and instructions for programmably selecting the enciphering algorithm from among the group consisting essentially of an F enciphering algorithm, a DES enciphering algorithm, and a BONUS enciphering algorithm.

48

35. (Twice amended) [The system of Claim 21,] A system for privately communicating communications signals over a wireless communications network, comprising:

a first communications controller at a first location;

a first signal processing circuit within said first communications controller circuit at the first location for processing communications signals to form processed communication signals and further for enciphering said processed communication signals;

a first transceiver associated at said first location with said first communications controller for transmitting said enciphered and processed communication signals between said first location and a second location;

B8 cont

a second communications controller circuit at the second location for controlling communications at said second location;

a second transceiver associated at the second location with said second communications circuit for receiving said enciphered and processed communication signals from said first transceiver;

a second signal processing circuit within said second communications controller circuit at the second location for deciphering said received enciphered and processed communication signals, said second signal processing circuit further for processing said deciphered and processed communication signals;

wherein said second communications controller circuit further comprises circuitry and instructions for embedding **[said]** a deciphering algorithm within said second signal processing circuit after first manufacturing said second communications controller circuit.

49

B8 cont

36. **(Once amended)** The system of Claim 35 **[31]**, wherein said deciphering algorithm comprises an F deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using an F enciphering algorithm.

37. **(Once amended)** The system of Claim 35 **[31]**, wherein said deciphering algorithm comprises a DES deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using an DES enciphering algorithm.

38. **(Once amended)** The system of Claim 35 **[31]**, wherein said deciphering algorithm comprises a BONUS deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using an BONUS enciphering algorithm.

39. **(Once amended)** The **[method]** **system** of Claim 35 **[31]**, wherein said **[enciphering]** deciphering algorithm **[embedding step]** comprises **[the step of embedding]** a DECT standard enciphering algorithm **[in said first signal processing circuit]** **embedded within said second signal processing circuit for deciphering communications signals first enciphered using a DECT enciphering algorithm**.

50

40. (Once amended) [The system of Claim 23,] A system for privately communicating communications signals over a wireless communications network, comprising:

a first communications controller at a first location;

a first signal processing circuit within said first communications controller circuit at the first location for processing communications signals to form processed communication signals and further for enciphering said processed communication signals;

B8 cont

a first transceiver associated at said first location with said first communications controller for transmitting said enciphered and processed communication signals between said first location and a second location;

a second communications controller circuit at the second location for controlling communications at said second location;

a second transceiver associated at the second location with said second communications circuit for receiving said enciphered and processed communication signals from said first transceiver;

a second signal processing circuit within said second communications controller circuit at the second location for deciphering said received enciphered and processed communication signals, said second signal processing circuit further for processing said deciphered and processed communication signals; and

further comprising circuitry and instructions within said first signal processing circuit for authenticating communications between said first location and said second location:

instructions within said first communications controller circuit for generating a first location identifier;

51

receiving circuitry associated with said first communications controller for receiving a randomly generated number from said second location;

privacy instructions embedded within said first signal processing circuit for employing a privacy function on said randomly generated number and said first location identifier **[at said]** to generate an enciphered value; and

communications circuitry for directing said enciphered value to said second communications controller circuit.

B8 cont

41. **(Twice amended)** The system of Claim **40** **[21]**, further comprising within said second communications controller circuit instructions for authenticating **[said]** generated authentication signals from said first location said authenticating instructions, comprising:

identifier generating instructions for generating **[said]** **a** first location identifier;

random number generating instructions for randomly generating **[said]** **a** randomly generated number;

privacy function instructions for transforming said randomly generated number and said first location identifier into an expected enciphered value;

receiving circuitry for receiving said enciphered value from said first location;

comparing instructions for comparing said expected enciphered value to said enciphered value; and

authentication generating instructions for generating a authentication signal in the event that said expected enciphered value matches said enciphered value.

52

42. (Once amended) [The system of Claim 21,] A system for privately communicating communications signals over a wireless communications network, comprising:

a first communications controller at a first location;

a first signal processing circuit within said first communications controller circuit at the first location for processing communications signals to form processed communication signals and further for enciphering said processed communication signals;

a first transceiver associated at said first location with said first communications controller for transmitting said enciphered and processed communication signals between said first location and a second location;

a second communications controller circuit at the second location for controlling communications at said second location;

a second transceiver associated at the second location with said second communications circuit for receiving said enciphered and processed communication signals from said first transceiver;

a second signal processing circuit within said second communications controller circuit at the second location for deciphering said received enciphered and processed communication signals, said second signal processing circuit further for processing said deciphered and processed communication signals; and

further comprising logic circuitry for XOR-ing said enciphered and processed communication signals with clear processed communication signals for preventing propagation of single bit errors that arise during enciphering from beyond the location at which they occur from said first signal processing circuit to said second signal processing circuit.

B8 cnt

43. **(Once amended)** A communications controller circuit for privately communicating communication signals over a wireless communications network, comprising:

a signal processing circuit within said communications controller circuit for processing communications signals to form processed communication signals and further **for** enciphering said processed communication signals; and

a transceiver associated with said communications controller circuit for transmitting said enciphered and processed communication signals from said communications controller circuit.

47. **(Once amended)** [The controller circuit of Claim 45,] **A communications controller circuit for privately communicating communication signals over a wireless communications network, comprising:**

a signal processing circuit within said communications controller circuit for processing communications signals to form processed communication signals and further for enciphering said processed communication signals; and

a transceiver associated with said communications controller circuit for transmitting said enciphered and processed communication signals from said communications controller circuit; and

further comprising an enciphering algorithm embedded within said signal processing circuit for enciphering said processed communication signals;

wherein said signal processing circuit further comprises circuitry and instructions for embedding said enciphering algorithm in said signal processing circuit after manufacturing said communications controller circuit.

53

48. **(Once amended)** The controller circuit of Claim **47** **[43]**, wherein said signal processing circuit comprises circuitry and instructions for embedding an F enciphering algorithm in said signal processing circuit.

49. **(Once amended)** The controller circuit of Claim **47** **[43]**, wherein said signal processing circuit comprises circuitry and instructions for embedding a DES enciphering algorithm in said signal processing circuit.

B9 cont

50. **(Once amended)** The controller circuit of Claim **47** **[43]**, wherein said signal processing circuit comprises circuitry and instructions for embedding a BONUS enciphering algorithm in said signal processing circuit.

56

39 not

51. **(Once amended) [The controller circuit of Claim 43,] A communications controller circuit for privately communicating communication signals over a wireless communications network, comprising:**

a signal processing circuit within said communications controller circuit for processing communications signals to form processed communication signals and further for enciphering said processed communication signals; and

a transceiver associated with said communications controller circuit for transmitting said enciphered and processed communication signals from said communications controller circuit;

wherein said signal processing circuit comprises circuitry and instructions for enciphering said processed communication signals in said signal processing circuit by programmably selecting an enciphering algorithm.

52. **(Once amended)** The controller circuit of Claim **51** **[45]**, wherein said signal processing circuit further comprises circuitry and instructions for programmably selecting the enciphering algorithm from among the group consisting essentially of an F enciphering algorithm a DES enciphering algorithm and a BONUS enciphering algorithm.

53. **(Once amended)** The controller circuit of Claim **43** **[48]**, further comprising a deciphering algorithm embedded within **[said]** **a** second signal processing circuit for deciphering said processed communication signals.

57

54. **(Once amended)** The controller circuit of Claim 53 **[49]**, wherein said second communications controller circuit further comprises circuitry and instructions for embedding said deciphering algorithm within said second signal processing circuit after manufacturing said second communications controller circuit.

B2 cont

55. **(Once amended)** The controller circuit of Claim 53 **[50]**, wherein said deciphering algorithm comprises an F deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using an F enciphering algorithm.

56. **(Once amended)** The controller circuit of Claim 53 **[51]**, wherein said deciphering algorithm comprises a DES deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using a DES enciphering algorithm.

57. **(Once amended)** The controller circuit of Claim 53 **[51]**, wherein said deciphering algorithm comprises a BONUS deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using a BONUS enciphering algorithm.

58

58. **(Once amended) [The controller circuit of Claim 43,]** **A communications controller circuit for privately communicating communication signals over a wireless communications network, comprising:**

a signal processing circuit within said communications controller circuit for processing communications signals to form processed communication signals and further for enciphering said processed communication signals; and

a transceiver associated with said communications controller circuit for transmitting said enciphered and processed communication signals from said communications controller circuit; and

B9 cont

further comprising circuitry and instructions within said signal processing circuit for authenticating communications between **[said]** **a** location and **[said]** **a** second location:

instructions within said communications controller circuit for generating a location identifier;

receiving circuitry associated with said communications controller for receiving a randomly generated number from said second location;

privacy instructions embedded within said signal processing circuit for employing a privacy function on said randomly generated number and said location identifier **[at said]** to generate an enciphered value; and

communications circuitry for directing said enciphered value to **[said]** **a** second communications controller circuit **at said second location**.

59

59. **(Once amended)** The controller circuit of Claim 58 **[54]**, further comprising within said second communications controller circuit instructions for authenticating said generated authentication signals from said location, said **[authenticating]** instructions[,] comprising:

B9 cont

identifier generating instructions for generating **[said]** a location identifier;

random number generating instructions for randomly generating **[said]** a randomly generated number;

privacy function instructions for transforming said randomly generated number and said location identifier into an expected enciphered value;

receiving circuitry for receiving **[said]** an enciphered value from said location;

comparing instructions for comparing said expected enciphered value to said enciphered value; and

authentication generating instructions for generating an authentication signal in the event that said expected enciphered value matches said enciphered value.

60

60. **(Once amended) [The controller circuit of Claim 41,]** **A communications controller circuit for privately communicating communication signals over a wireless communications network, comprising:**

a signal processing circuit within said communications controller circuit for processing communications signals to form processed communication signals and further for enciphering said processed communication signals; and

a transceiver associated with said communications controller circuit for transmitting said enciphered and processed communication signals from said communications controller circuit; and

further comprising logic circuitry for XOR-ing said enciphered and processed communication signals with clear processed communication signals for preventing propagation of single bit errors beyond **[the]** **a** location at which they occur as a consequence of the enciphering process from said signal processing circuit to **[said]** **a** second signal processing circuit.

B7 cnt

61